DETAILED ACTION

1. This action in responsive to the communication filed on 5/18/09   .

2. Claims 1, 5-8, 10 are allowed.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with the applicant representative, Mr. Eustace P. Isidore (Reg. No. 56,104) on 08/20/09. During the telephone conference, Mr. Isidore has agreed and authorized examiner to amend claim 1 to overcome the 112, 2nd issue.

CLAIM:

a. <u>Referring to claim 1</u>:

Please replace claim 1 as follows:

A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices, wherein said non-public, secure value is a secret number;

transmitting a first copy of said secret number via a secure communication medium to said credential server;

hashing a second copy of said secret number with a public key from said endorsement key pair;

combining a first hash result from said hashing step with the public key to create an endorsement key (EK);

transmitting said EK to said credential server to initiate a credential process;

verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during

manufacture of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server, said verifying step further comprising:

receiving said EK from said device at the credential server,

calculating an expected hash value by hashing the public key within the received

EK with the first copy of said secret number received during <u>said transmitting step</u>,

comparing the first hashed value from within the EK with the expected

hash value, and

confirming said EK is from a valid device when said comparing step

results in a match; and

in response to confirming said EK is from a valid device, inserting an

endorsement certificate into said device to indicate that said device is an approved

device by an original equipment manufacturer (OEM) of the device.

Response to Arguments

3. Applicant's arguments, filed May 18, 2008 (Appeal Brief) have been fully

considered and are persuasive.

Allowable Subject Matter

4. Claims 1, 5-8, 10 are allowed.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Nirav Patel whose telephone number is 571-272-5936.

The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP
08/20/09
/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435